

Technical Cybersecurity

From the Outside In

Remote Exploitation

THE FANCIEST APPROACH

- ▶ Break into systems from the outside
- ▶ Overcome the perimeter without inside involvement
- ▶ Deploy executable code to establish a foothold

Password Cracking

PASSWORDS ARE ENCRYPTED

- ▶ We can still crack them
- ▶ If we can acquire lists of passwords, we can attempt to brute-force the passwords via known algorithms
- ▶ Becoming more and more feasible vs. complex passwords every day
- ▶ GPU acceleration

Credential Capture & Cracking

SNIFFING FOR TRAFFIC W/ CREDENTIALS

- ▶ We can sniff for passwords on network traffic
- ▶ Extract passwords (or hashes) from traffic for later use
- ▶ Man-in-the-middle insertion

We'll start with remote
exploitation.